Your 802.11 Wireless Network has No Clothes*

William A. Arbaugh
Narendar Shankar
Y.C. Justin Wan
Department of Computer Science
University of Maryland
College Park, Maryland 20742

March 30, 2001

Abstract

The explosive growth in wireless networks over the last few years resembles the rapid growth of the Internet within the last decade. During the beginning of the commercialization of the Internet, organizations and individuals connected without concern for the security of their system or network. Over time, it became apparent that some form of security was required to prevent outsiders from exploiting the connected resources. To protect the internal resources, organizations usually purchased and installed an Internet firewall.

We believe that the current wireless access points present a larger security problem than the early Internet connections. A large number of organizations, based on vendor literature, believe that the security provided by their deployed wireless access points is sufficient to prevent unauthorized access and use. Unfortunately, nothing could be further from the truth. While the current access points provide several security mechanisms, our work combined with the work of others show that *ALL* of these mechanisms are completely in-effective. As a result, organizations with deployed wireless networks are vulnerable to unauthorized use of, and access to, their internal infrastructure.

1 Introduction

Organizations are rapidly deploying wireless infrastructures based on the IEEE 802.11 standard [1]. Unfortunately, the 802.11 standard provides

only limited support for confidentiality through the wired equivalent privacy (WEP) protocol which contains significant flaws in the design [2, 3]. Furthermore, the standards committee for 802.11 left many of the difficult security issues such as key management and a robust authentication mechanism as open problems. As a result, many of the organizations deploying wireless networks use either a permanent fixed cryptographic variable, or key, or no encryption what so ever. This fact, coupled with the fact that wireless networks provide a network access point for an adversary (potentially beyond the physical security controls of the organization), creates a significant long term security problem. Compounding this is the fact that the access control mechanisms available with current access points contain serious flaws such that an adversary can easily subvert them.

Organizations over the last few years have expended a considerable effort to protect their internal infrastructure from *external* compromise. As a result, the organizations have canalized their external network traffic through distinct openings protected by firewalls. The idea is simple. By limiting external connections to a few well protected openings, the organization can better protect itself. Unfortunately, the deployment of a wireless network opens a "back door" into the internal network that permits an attacker access beyond the physical security perimeter of the organization. As a result, the attacker can implement the "parking lot" attack, see figure 1, where the attacker sits in the organization's parking lot and accesses hosts on the internal network. Ironically in some cases, the existence of the firewall may make the organization's hosts more vulnerable to the attacker because of the mistaken premise that the hosts are immune from attack and potential compromise.

This paper describes the flaws in the two access control mechanisms that exist in access points built using Orinoco/Lucent 802.11 Wavelan PCMCIA cards, and a simple eavesdropping attack against the 802.11 specified shared key authentication mechanism. Exploiting these flaws when encryption is not enabled permits an adversary immediate access to the wireless network and most likely the organization's local area network as well. The use of encryption prevents an adversary from gaining immediate access, but combining our attacks with the weaknesses found in WEP by others provides such access [2, 3].

The next section presents a short overview of the 802.11 wireless standard. This is followed an overview of the 802.11 security mechanisms, and Lucent's proprietary extension for access control. The next section describes attacks against the only two access control mechanisms available in most current access points, and an attack against the 802.11 standard shared key

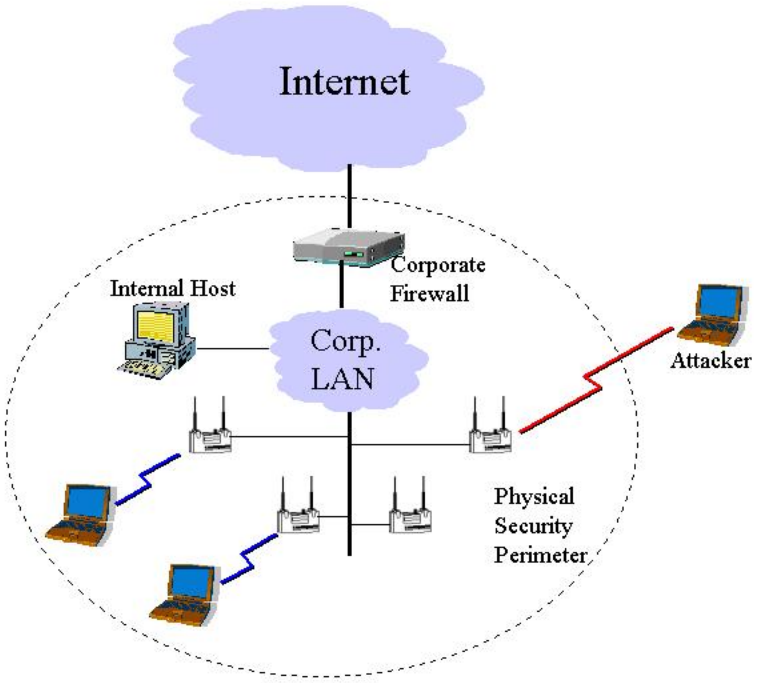

Figure 1: The Parking Lot attack

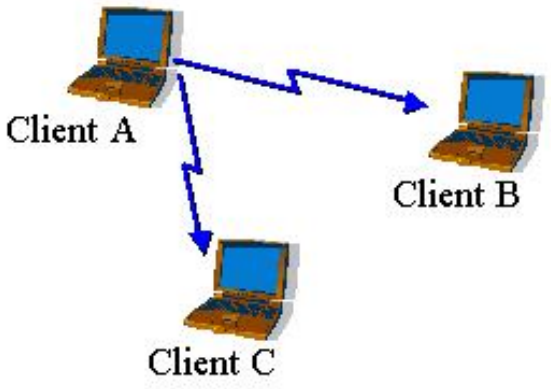

Figure 2: Example ad-hoc network

authentication mechanism. Finally, we conclude the paper with recommendations for organizations with operational wireless networks.

2 802.11 Wireless Networks

802.11 wireless networks operate in one of two modes- *ad-hoc* or *infrastructure* mode. The IEEE standard defines the *ad-hoc* mode as Independent Basic Service Set (IBSS), and the *infrastructure* mode as Basic Service Set (BSS). In the remainder of this section, we explain the differences between the two modes and how they operate.

In *ad hoc* mode, each client communicates directly with the other clients within the network, see figure 2. *ad-hoc* mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate. If a client in an *ad-hoc* network wishes to communicate outside of the cell, a member of the cell *MUST* operate as a gateway and perform routing.

In *infrastructure* mode, each client sends all of it's communications to a central station, or access point (AP). The access point acts as an ethernet bridge and forwards the communications onto the appropriate network– either the wired network, or the wireless network, see figure 3.

Prior to communicating data, wireless clients and access points must establish a relationship, or an *association*. Only after an *association* is established can the two wireless stations exchange data. In *infrastructure*

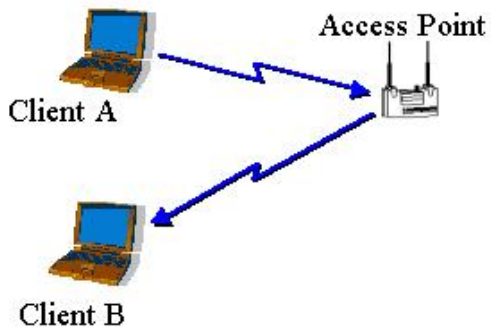

Figure 3: Example infrastructure network

mode, the clients associate with an access point. The association process is a two step process involving three states:

1. *Unauthenticated and unassociated*,
2. *Authenticated and unassociated*, and
3. *Authenticated and associated*.

To transition between the states, the communicating parties exchange messages called management frames.

We will now walk through a wireless client finding and associating with an access point. All access points transmit a *beacon* management frame at fixed interval. To associate with an access point and join a BSS, a client listens for beacon messages to identify the access points within range. The client then selects the BSS to join in a vendor independent manner. For instance on the Apple Macintosh, all of the network names (or service set identifiers (SSID)) which are usually contained in the beacon frame are presented to the user so that they may select the network to join. A client may also send a *probe* request management frame to find an access point affiliated with a desired SSID. After identifying an access point, the client and the access point perform a mutual authentication by exchanging several management frames as part of the process. The two standardized authentication mechanisms are described in sections 3.2 and 3.3. After successful authentication, the client moves into the second state, *authenticated and*

unassociated. Moving from the second state to the third and final state, *authenticated and associated*, involves the client sending an *association* request frame, and the access point responding with an *association* response frame.

After following the process described in the previous paragraph, the client becomes a peer on the wireless network, and can transmit data frames on the network.

3 802.11 Standard Security Mechanisms

The 802.11 standard provides several mechanisms intended to provide a secure operating environment[1]. In this section, we describe each of these mechanisms as well as a Lucent proprietary method.

3.1 Wired Equivalent Privacy protocol

The Wired Equivalent Privacy (WEP) protocol was designed to provide confidentiality for network traffic using the wireless protocol. The details of the algorithm used for WEP are beyond the scope of this paper. However, work by Walker and more recently by Borisov, Goldberg, and Wagner demonstrates that WEP, when used without a short key period, provides limited confidentiality [2, 3], and possible misuse of the network.

3.2 Open System Authentication

Open system authentication is the default authentication protocol for 802.11. As the name implies, open system authentication authenticates anyone who requests authentication. Essentially, it provides a NULL authentication process. Experimentation has shown that stations do perform a mutual authentication using this method when joining a network, and our experiments show that the authentication management frames are sent in the clear even when WEP is enabled.

3.3 Shared Key Authentication

Shared key authentication uses a standard challenge and response along with a shared secret key to provide authentication. The station wishing

[1] At least one major vendor has implemented, authentication via the Extensible Authentication Protocol (EAP) [4]. Since the exact protocol used is unknown at this time, we can not provide any additional information about it, nor can we determine the level of security provided by it.

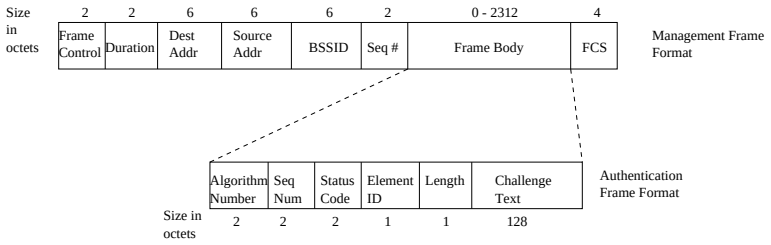

Figure 4: Authentication Management Frame

to authenticate, the *initiator*, sends an authentication request management frame indicating that they wish to use "shared key" authentication. The recipient of the authentication request, the *responder*, responds by sending an authentication management frame containing 128 octets of challenge text to the *initiator*. The challenge text is generated by using the WEP pseudo-random number generator (PRNG) with the "shared secret" and a random initialization vector (IV)[2]. Once the *initiator* receives the management frame from the *responder*, they copy the contents of the challenge text into a new management frame body. This new management frame body is then encrypted with WEP using the "shared secret" along with a new IV selected by the initiator. The encrypted management frame is then sent to the *responder*. The *responder* decrypts the received frame and verifies that the 32-bit CRC integrity check value (ICV) is valid, and that the challenge text matches that sent in the first message. If they do, then authentication is successful. If the authentication is successful, then the initiator and the responder switch roles and repeat the process to ensure mutual authentication. The entire process is shown in figure 5, and the format of an authentication management frame is shown in figure 4. The format shown is used for all authentication messages.

The value of the status code field is set to zero when successful, and to an error value if unsuccessful. The element identifier identifies that the challenge text is included. The length field identifies the length of the challenge text and is fixed at 128. The challenge text includes the random challenge string. Table 1 shows the possible values and when the challenge text is included based on the message sequence number.

[2]The IV is always sent in the clear as part of a WEP protected frame.

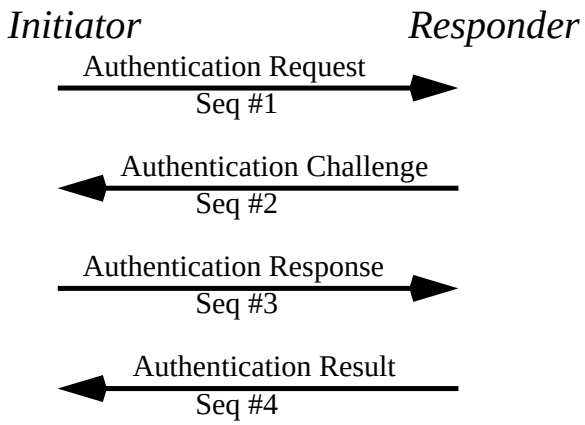

Figure 5: Mutual Station Authentication using shared keys

Sequence number	**Status code**	**Challenge text**	**WEP used**
1	Reserved	Not present	No
2	Status	Present	No
3	Reserved	Present	Yes
4	Status	Not Present	No

Table 1: Message Format based on Sequence Number

3.4 Closed Network Access Control

Lucent has defined a proprietary access control mechanism called *Closed Network* [5]. With this mechanism, a network manager can use either an *open* or a *closed* network. In an open network, anyone is permitted to join the network. In a closed network, only those clients with knowledge of the network name, or SSID, can join. In essence, the network name acts as a *shared secret*.

3.5 Access Control Lists

Another mechanism used by vendors (but not defined in the standard) to provide security is the use of access control lists based on the ethernet MAC address of the client. Each access point can limit the clients of the network to those using a listed MAC address. If a client's MAC address is listed, then they are permitted access to the network. If the address is not listed, then access to the network is prevented.

3.6 Key Management

Key management is a misnomer with respect to 802.11 as it is left as an exercise for vendors. As a result, only a few of the major vendors have implemented any form of key management or key agreement in their high-end products. Unfortunately, none of the vendors provide sufficient information to determine the level of assurance provided by their product. Worse, in some cases, the details that are available indicate that the vendors "solution" worsens the problem by using protocols with well-known vulnerabilities, e.g. un-authenticated Diffie-Hellman key agreement.

The 802.11 standard does, however, provide for two methods for using WEP keys. The first provides a window of four keys. A station or AP can decrypt packets enciphered with any one of the four keys. Transmission, however, is limited to one of the four manually entered keys– the *default key*. The second method is called a key mappings table. In this method, each unique MAC address can have a separate key. The size of a key mappings table should be at least ten entries according to the 802.11 specification. The maximum size, however, is likely chip-set dependent. The use of a separate key for each user mitigates the cryptographic attacks found by others, but enforcing a reasonable key period remains a problem as the keys can only be changed manually.

4 Weaknesses in Current Access Control Mechanisms

This section describes the weaknesses in the access control mechanisms of currently deployed wireless network access points.

4.1 Lucent's proprietary access control mechanism

In practice, security mechanisms based on a shared secret are robust provided the secrets are well-protected in use and when distributed. Unfortunately, this is not the case with Lucent's proprietary access control mechanism. Several management messages contain the network name, or SSID, and these messages are broadcast in the clear by access points and clients. The actual message containing the SSID depends on the vendor of the access point. The end result, however, is that an attacker can easily *sniff* the network name- determining the shared secret and gaining access to the "protected" network. This flaw exists even with WEP enabled because the management messages are broadcast in the clear.

4.2 Ethernet MAC Address Access Control Lists

In theory, access control lists provide a reasonable level of security when a strong form of identity is used. Unfortunately, this is not the case with MAC addresses for two reasons. First, MAC addresses are easily *sniffed* by an attacker since they MUST appear in the clear even when WEP is enabled, and second most all of the wireless cards permit the changing of their MAC address via software. As a result, an attacker can easily determine the MAC addresses permitted access via eavesdropping, and then subsequently masquerade as a valid address by programming the desired address into the wireless card– by-passing the access control and gaining access to the "protected" network.

5 Shared Key Authentication Flaw

The current protocol for shared key authentication is easily exploited through a passive attack by the eavesdropping of one leg of a mutual authentication. The attack works because of the fixed structure of the protocol (the only difference between different authentication messages is the random challenge), and the previously reported weaknesses in WEP [2, 3].

The attacker first captures the second and third management messages from an authentication exchange, see table 1. The second message contains the random challenge in the clear, and the third message contains the challenge encrypted with the shared authentication key. Because the attacker now knows the random challenge (*plaintext*, P), the encrypted challenge (*ciphertext*, C), and the public IV, the attacker can derive the pseudo-random stream produced using WEP, $WEP_{PR}^{K,IV}$, with the shared key, K, and the public initialization variable, IV, using equation 1.

$$WEP_{PR}^{K,IV} = C \oplus P \tag{1}$$

The size of the recovered pseudo-random stream will be the size of the authentication frame, see figure 4 because all elements of the frame are known: algorithm number, sequence number, status code, element id, length, and the challenge text. Furthermore, all but the challenge text will remain the same for ALL authentication responses.

The attacker now has all of the elements to successfully authenticate to the target network– without knowing the shared secret K. The attacker requests authentication of the access point it wishes to associate/join. The access point responds with an authentication challenge in the clear. The attacker, then, takes the random challenge text, R, and the pseudo-random stream, $WEP_{PR}^{K,IV}$, and computes a valid authentication response frame body by *XOR-ing* the two values together. The attacker then computes a new integrity check value (ICV) as described in Borisov et. al. [3, 6]. Now, the attacker responds with a valid authentication response message, and he associates with the AP and joins the network[3]. Utilizing the network when WEP is enabled, however, requires the attacker to implement the WEP attacks [2, 3].

6 Conclusions and Future Work

The combination of our results with those of Walker and Borisov et. al. demonstrates serious flaws in ALL of the security mechanisms used by the vast majority of access points supporting the IEEE 802.11 wireless standard. The end result is that ALL of the deployed 802.11 wireless networks are at risk of compromise– providing a network access point to internal networks beyond the physical security controls of the organization operating the network. Unfortunately, fixing the problem is not easy nor straight forward.

[3]We identified this flaw independently. After explaining it to Jesse Walker, we learned that the 802.11 committee was aware of the problem [6]

An interim short term mitigation (not a complete solution) is a robust key management system for WEP, and the use of higher level security mechanisms, e.g. IPsec. These mechanisms, however, just mitigate the problem until a new encapsulation algorithm is established by the IEEE 802.11 standards committee, and packet forgery will remain a problem until data authentication becomes standard.

The only good long term solution is a major overhaul of the current standard which may require replacement of current AP's (although in some cases a firmware upgrade may be possible). Fortunately, the 802.11 standards body is currently working on significant improvements to the standard [7]. However, it is too late for deployed networks and for those networks about to be deployed.

A number of vendors are now releasing high-end access points claiming that they provide an increase in security. Unfortunately, few of the products we have examined provide enough information to determine the overall assurance that the product will provide, and worse, several of the products that do provide enough information use un-authenticated Diffie-Hellman which suffers from a well-known *man in the middle* attack. The use of un-authenticated Diffie-Hellman introduces a greater vulnerability to the organization's network. The increase in risk occurs because an attacker can insert themself in the middle of the key exchange between the client and the access point– obtaining the session key, K. This is significantly worse than the current situation where the attacker must first determine the pseudo-random stream produced for a given key, K, and public IV, and then use the stream to forge packets.

7 Acknowledgments

The authors would like to thank Jesse Walker of the Intel Corporation, Mark Seiden of Securify, and Angelos Keromytis of the University of Pennsylvania for providing valuable comments on a draft of this work.

References

[1] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer(PHY) specification. IEEE Standard 802.11, 1997 Edition," 1997.

[2] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zi%p.

[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11." http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[4] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," Tech. Rep. RFC2284, Internet Engineering Task Force (IETF), March 1998.

[5] Lucent Orinoco, *User's Guide for the ORiNOCO Manager's Suite*, November 2000.

[6] J. Walker, "Overview of 802.11 security." http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3%-Overview-of-802-11-Security.ppt, March 2001.

[7] IEEE 802.11 Working Group. http://grouper.ieee.org/groups/802/11/index.html.